

Art Unit: ***

CLMPTO

04-01-02

MBL

CLAIMS

1- 15 CANCELED

CLAIM 16 AMENDED

16. A method of providing secure communication between a mobile node and a home domain using a foreign domain comprising:

transmitting a registration request from the mobile node to the home domain the request comprising an identity of a user of the mobile node in encrypted form and network routing information in non-encrypted form;

the home domain receiving and processing the registration request to generate a registration reply comprising one or more encryption keys for encrypting messages to be communicated between and among the mobile node home

Art Unit: ***

13 17. The method of claim 16, wherein transmitting a registration request from
14 the mobile node to the home domain comprises:
15 transmitting the registration request from the mobile node to the foreign
16 domain; and
17 transmitting the registration request from the foreign domain to the home
18 domain.

1 18. The method of claim 17, wherein transmitting the registration request from
2 the foreign domain to the home domain comprises establishing a secure
3 communications pathway between the foreign domain and the home domain.

1 19. The method of claim 17, wherein transmitting the registration request from
2 the foreign domain to the home domain comprises establishing a secure
3 communications pathway between the foreign domain and the mobile node.

1 20. The method of claim 17, wherein transmitting the registration request from
2 the foreign domain to the home domain comprises establishing a secure
3 communications pathway between the home domain and the mobile node.

1 21. The method of claim 16, wherein processing the registration request from
2 the mobile node within the home domain comprises decrypting the encrypted
3 form of the identity of the user.

1 22. The method of claim 16, wherein generating a registration reply comprises
2 encrypting at least one of the encryption keys.

1 23. The method of claim 22, wherein generating a registration reply comprises
2 encrypting the encryption keys for encrypting messages to be communicated
3 between the mobile node and the home domain, and between the mobile node
4 and the foreign domain.

Art Unit: ***

1 24. The method of claim 22, further comprising:

2 decrypting one or more of the encrypted encryption keys.

3 25. The method of claim 16, wherein generating the registration reply
4 comprises:

5 generating a first encryption key for encrypting messages to be

6 communicated between the mobile node and the home domain;

7 generating a second encryption key for encrypting messages to be

8 communicated between the foreign domain and the home domain;

9 and

10 generating a third encryption key for encrypting messages to be

11 communicated between the foreign domain and the mobile node.

1 26. The method of claim 22, wherein generating the registration reply

2 comprises encrypting at least one of the first and third encryption keys.

1 27. The method of claim 26, further comprising:

2 decrypting at least one of the encrypted first and third encryption keys.

1 28. The method of claim 16, wherein the registration reply includes:

2 encryption keys that are encrypted; and

3 encryption keys that are not encrypted.

1 29. The method of claim 28, further including:

2 extracting one or more of the encryption keys that are not encrypted from
3 the registration reply.

Art Unit: ***

- 1 30. The method of claim 28, further including:
2 extracting and decrypting one or more of the encryption keys that are
3 encrypted from the registration reply.

31-69 CANCELLED

- 1 70. A method of providing secure communications between an initiator and a
2 responder in a communications network, comprising:
3 dynamically establishing a security association between the initiator and
4 the responder.

- 1 71. The method of claim 70, further comprising:
2 negotiating the security association.

- 1 72. The method of claim 71, wherein negotiating the security association
2 comprises:
3 negotiating one or more security transforms to be used to provide secure
4 communications between the initiator and the responder.

- 5 73. The method of claim 71, wherein negotiating the security association
6 comprises:
7 proposing the number of transforms to be used to provide secure
8 communications between the initiator and the responder.

- 1 74. The method of claim 71, wherein negotiating the security association
2 comprises:
3 proposing the duration of at least a portion of the security association.

- 1 75. The method of claim 71, wherein negotiating the security association

Art Unit: ***

2 comprises:

3 proposing the type of transforms to be used to provide secure
4 communications between the initiator and the responder.

76 – 127 CANCELLED